**AMENDMENTS TO THE CLAIMS**

This listing of claims will replace all prior versions, and listing, of claims in the application:

Listing of Claims:

1. (currently amended) A method, comprising:

receiving an electronic mail message in a computer;

using the computer for displaying information about the electronic mail message;

using the computer for displaying all of first, second and third controls, where said first control causes the computer to ~~in a way that allows all of deleting~~delete the message without indicating whether ~~it is~~does represent a spam message or does not represent a spam message, the second control causes the computer to delete ~~deleting~~ the message while indicating that it does represent a ~~is~~ spam message, and the third control causes the computer to delete~~or deleting~~ the message while indicating that ~~it is~~the message does not represent a spam message.

2. (currently amended) A method as in claim 1 further comprising using the computer for storing a database of spam likelihood, and wherein said deleting ~~while indicating~~ using said second and third controls causes changes to ~~updates~~ information in the database of spam likelihood, and said deleting using said first control does not cause changes to information in said database of spam likelihood.

3. (currently amended) A method as in claim 1 wherein said deleting using said second and third controls ~~while indicating updates~~ changes at least one rules ~~in~~ a rules database, and said deleting using said first control does not cause changes of said rules in said rules database.

4. (Previously Presented) A method as in claim 3 wherein said rules include information about fields from said electronic mail message.

5. (currently amended) A method as in claim ~~3~~ 4 wherein said fields from said electronic mail message which are used to change said rules include at least a sender of the e-mail message, text of the e-mail message, and a subject of the e-mail message, and wherein each of said fields are used as parts of rules in said rules database.

6. (currently amended) A method as in claim 5 wherein said fields from said electronic mail message which are used to change said rules also include a domain of a sender of the e-mail message.

7. (currently amended) A method as in claim 3, wherein said fields from said electronic mail message which are used to change said rules include links within the e-mail message, where certain links in an email message represent that the electronic mail message is more likely to represent spam.

8-13 (cancelled)

14. (currently amended) A computer program product, comprising a computer usable medium having computer readable program code embodied therein, said computer readable program code adapted to be executed to implement ~~An~~ e-mail program, comprising:

an email receiving part that receives emails;

a display ~~portion~~ output which produces an output which displays a plurality of said e-mails ; and also displays and accepts input from a plurality of controls including both of:

~~at least~~ a first control which selects deleting an e-mail while indicating that said e-mail is spam and reports information indicative of said email to a spam determining database, and

a second control which selects deleting an e-mail while indicating that said e-mail is not spam and does not report information indicative of said email to said spam determining database;

a database update part that adds information indicative of said information reported by said first control and said second control to said spam determining database; and

a spam determining part that analyzes said emails received by said email receiving part based on information in said database as updated by said database update part .

15. (currently amended) A program as in claim 14, ~~further comprising~~ ~~displaying~~ wherein said display output displays a likelihood of spam coefficient which indicates a numerical percentage ~~, on a weighted scale, a~~ likelihood that the associated message represents spam.

16. (currently amended) A program as in claim 14, wherein said display output further ~~comprising displaying a~~ displays a third control which ~~allows~~ selects deleting an e-mail without indicating or not indicating whether said e-mail represents spam.

17-20 (cancelled)

21. (currently amended) A method, comprising:

using a computer for determining a plurality of characteristics of an unwanted electronic message;

using the computer for forming a list with said plurality of characteristics;

using the computer for receiving an incoming electronic message, and forming a ~~numerical~~ score of ~~an~~ the incoming message by comparing said incoming message with said list and determining commonalities between said incoming message and said list, wherein said comparing comprises determining a domain of the sender, and comparing said domain a the sender with information about spam messages in the database, to obtain a higher probability of spam when information about all senders from a specific domain in said database represent spam, and to represent a lower

probability of spam when some senders from said domain in said database represent spam and other senders from said domain in said database do not represent spam;

using the computer for defining said incoming message as likely being unwanted if said ~~numerical~~ score is within a predetermined range; and

using the computer for taking an action to restrict said message based on said defining.

22 (cancelled)

23. (currently amended) ~~A method~~An apparatus, comprising:

a computer which receives ~~obtaining~~ an electronic mail message over an electronic channel;

said computer automatically comparing said electronic mail message with information indicative of undesired electronic mail messages; and

said computer producing a user interface that displays information about said electronic mail message, and which user interface allows a selection to all of:

A) delete the message without indicating whether or not the message represents spam,

B) delete the message while indicating that the message does indicate spam, and using information from a first message deleted as spam to change said information indicative of undesired electronic mail messages; and

~~or~~ C) delete the message while indicating that the message does not indicate spam, and using information from a second message deleted as spam to change said information indicative of desired electronic mail messages .

24. (Currently amended) ~~A method~~An apparatus as in claim 23, further comprising a database of information indicating likelihood of spam, and wherein said delete while indicating that the message does indicate spam ~~updates~~ changes information in said database.

25. (New) A method as in claim 2, further comprising using the computer for displaying said spam likelihood as a numerical percentage indicating a likelihood that the message represents spam.

26. (New) A method as in claim 2, further comprising displaying a message in a color, where the color represents a likelihood that the message represents spam.

27. (New) A method as in claim 3, further comprising using the computer to automatically classify an incoming message as a spam message, or not as a spam message, based on said rules in said database as changed by said first and second controls .

28. (New) A method as in claim 27, further comprising displaying the messages along with an indication of whether they have been classified to represent spam or not to represent spam.

29. (New) A method as in claim 27, further comprising displaying messages that have not been classified to represent spam in a first view, and displaying messages that do represent spam in a second view.

30. (New) A method as in claim 3, wherein one of said fields from said electronic mail message includes a domain of the sender, said domain being used to change said rules in said database.

31. (New) A method as in claim 30, wherein the first rule is changed to represent a higher probability of spam when all senders from a specific domain represent spam, and to represent a lower probability of spam when some senders from said domain represent spam and other senders from said domain do not represent spam.

32. (New) A method as in claim 3, wherein said changes to said rules in said database uses multiple different techniques to analyze the message and to determine that the message likely represents a spam message.

33. (New) A product as in claim 14, further comprising a display part which displays the messages analyzed by said spam determining part along with an indication of whether they have been classified to represent spam or not to represent spam.

34. (New) A product as in claim 27, further comprising displaying messages that have not been classified to represent spam in a first view, and displaying messages that do represent spam in a second view that is wholly separate from the first view.

35. (New) A product as in claim 14, wherein said database update part uses a domain of the sender to change said rules in said database.

36. (New) A product as in claim 35, wherein the first rule is changed to represent a higher probability of spam when all senders from a specific domain represent spam, and to represent a lower probability of spam when some senders from said domain represent spam and other senders from said domain do not represent spam.

37. (New) An apparatus as in claim 23, further comprising displaying a message in a color, where the color represents a likelihood that the message represents spam.

38. (New) A method as in claim 23, wherein said computer automatically classifies an incoming message as being a spam message, or not being a spam

message, based on said information indicative of undesired electronic mail messages as updated by said first and second messages.

39. (New) A method as in claim 38, wherein said computer produces an output that displays the messages along with an indication of whether they have been classified to represent spam or not to represent spam.

40. (New) A method as in claim 38, wherein said computer produces an output that displays the messages that have not been classified to represent spam in a first view, and displaying messages that do represent spam in a second view that is separate from said first view.

41. (New) A method as in claim 38, wherein said information from said first and second messages includes a domain of the sender, said domain being used to change said information indicative of undesired electronic mail messages.

42. (New) method as in claim 41, wherein the first rule is changed to represent a higher probability of spam when all senders from a specific domain represent spam, and to represent a lower probability of spam when some senders from said domain represent spam and other senders from said domain do not represent spam.

43. (New) A method as in claim 38, wherein said changes to said rules in said database uses multiple different techniques to analyze the message and to determine that the message likely represents a spam message.